Microsoft®

Windows.net™

Server Family

Security in IIS 6.0

Asim Mitra
Program Manager
Internet Information Services
Microsoft Corporation

Field Reviewer: Jeff Williams

Roadmap

- Is IIS 5.0 a secure web server?
  - What we learnt
- IIS 6.0 security boost
  - Lessons implemented
  - Security features for the platform
- Key takeaways

Is IIS 5.0 a secure web server?

- Code Red and Nimda hit customers hard
- What we learnt
  - Windows® 2000 Installed As An Application Server – Huge attack surface
  - Soft Defaults
  - High Privilege Accounts
  - No automated way to install patches
    - Result: Fixes out for months but not uniformly applied
      - Unicode Fix (Nimda) since October 2000
      - Index Server Fix (Nimda, Code Red) since June 2001
- Many customers survived Code Red & Nimda
- IIS Lockdown Wizard & URLSCAN for IIS

IIS 6.0 Security Boost

- Lessons implemented
  - Reduced attack surface
  - Code security
  - Secure defaults
  - Defense in depth
  - Improved ASP security
  - Lower privilege accounts
  - Improved patch management
- Security features for the platform
  - Application isolation
  - FTP user isolation
  - Passport authentication
  - URL authorization

Reduced Attack Surface

- IIS is not installed by default
  - As well as 20+ other services
- Server Lockdown: Serve HTM files only
  - Only Web service gets installed
  - IsapiRestrictionList
  - CGIRestrictionList
  - Template-based feature activation

Feature Activation Wizard/Console

demo

Code Security

- Buffer overflow checks
  - Automated in the Windows build environment
    - Prefix: Bound violations, return value checking, memory management
    - Prefast: Buffer overflow, HRESULT violation
  - Visual C++® compiler supported (/Gs)
- Revised canonicalization
  - NTFS stream outlawed
    - Bar.asp::$DATA
    - Bar.asp.
  - \\?\ (turns off createfile() canonicalization)
- Old legacy code removed

Secure Defaults

- No executable VDirs
  - /SCRIPTS and /MSADC
- Secure timeouts and limits
  - 16k request limit (128K in Windows 2000)
- ACL's on
  - Command line files
    - Deny for "Web Anonymous Users" on all .EXE in system32
  - Content
    - Deny write for "Web Anonymous Users" group
  - Logfiles
  - Custom error directory
  - On cache directories
    - Persistent ASP template cache
    - Compression cache
- Check if file exists

Defense in depth

- Feature activation wizard/console
- URLSCAN
  - DenyHeaders
  - DenyVerbs
  - DenyUrlSequences
- ExtensionRestrictionList

ASP security improvements

- F5 attack prevention
- 4MB response buffer limit
- Hang detection
- AspEnableParentPath = FALSE

Lower privilege accounts

- IIS 6.0 Worker processes run as NetworkService by default
  - LocalSystem
    - In Administrator's group
    - 22 Privileges including TCB (Trusted Computer Base)
  - NetworkService
    - User
    - 5 Privileges
  - Worker process identity is completely configurable
- Application considerations

Configurable Worker Process Identity

demo

Patch Management

- Patches installed without any service interruption
- Stay secure with AutoUpdate
  - Just notify patch availability
  - Download patch and notify
  - Scheduled Install: Download patch and install at a time decided by the administrator
  - Immediate Install (not yet implemented) : with no service interruption
- Windows Update Corporate Edition

Security through isolation

- New Worker process architecture
  - True isolation, sandboxing and QoS
- FTP user isolation
- Delegation- works across all protocols
  - Security through constrained delegation

Application isolation

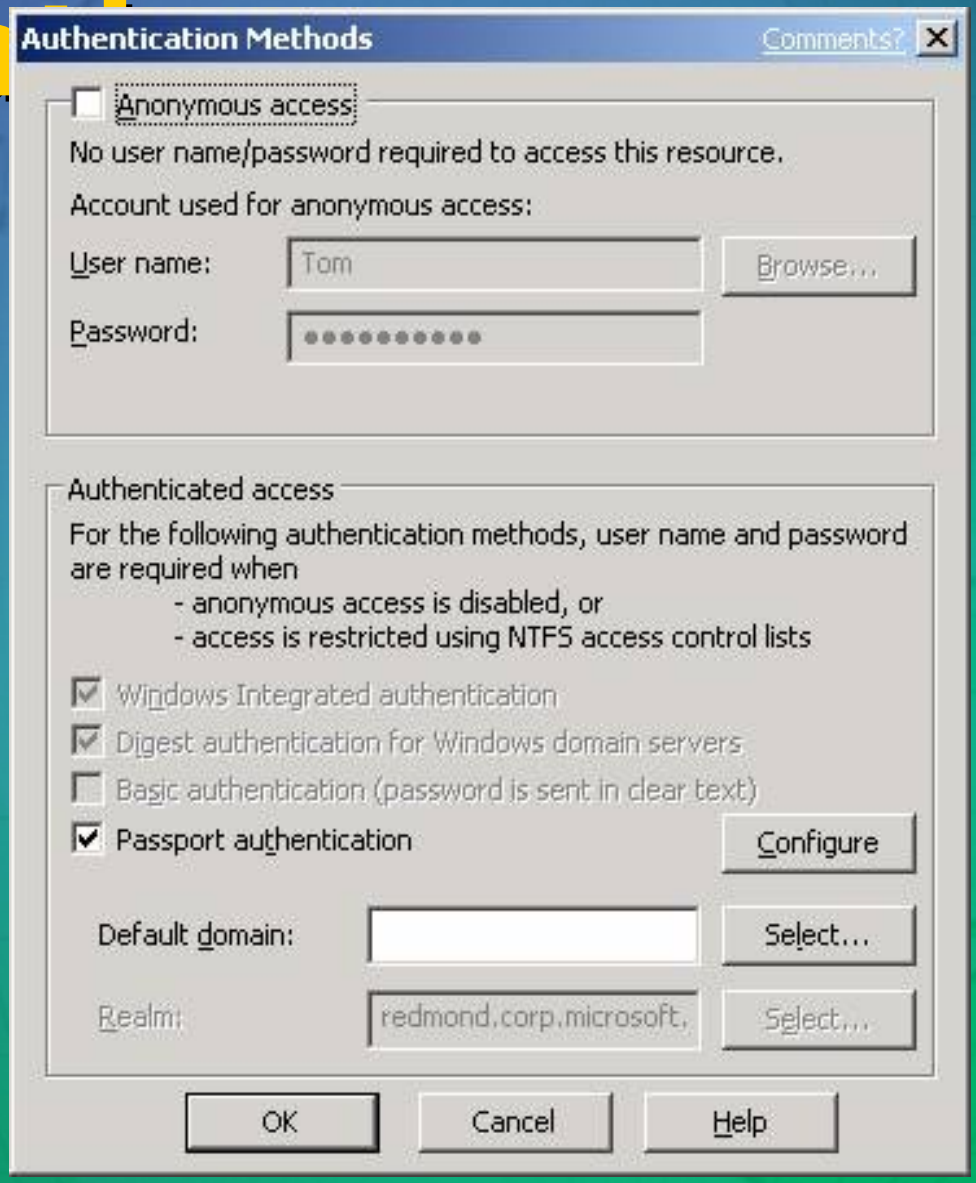
- True sandboxing
  - Worker processes can be confined to their root directory through ACL's
    - Specific Resources need to be ACL'd for the particular Worker process identity and anonymous account
      - Content
    - Common resources are ACL'd for the IIS_WPG group
      - Metabase
      - Registry
      - Cache directories

FTP user isolation

- FTP server 6.0 included in .net server
- Isolation levels
  - Compatibility / no isolation
  - Small business / stand alone isolation
  - Enterprise isolation using AD integration

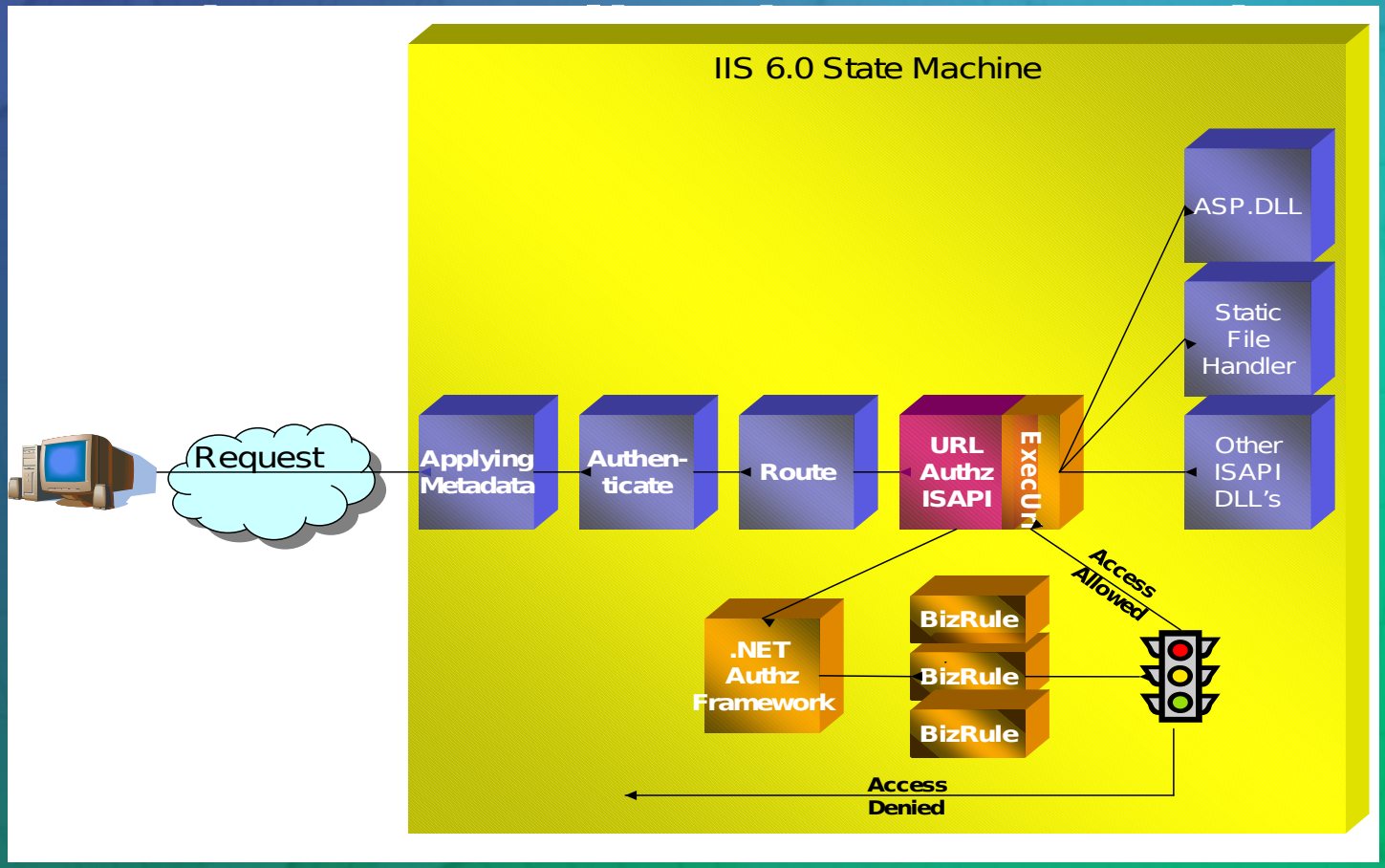
Passport Authentica

- Integrated with .NET server
- Can ACL resources with passport accounts
- Map passport credentials with AD accounts



URL Authorization (new)

- ACLs are too static and object driven
-



Key takeaways

- Committed to Windows 2000 (IIS 5) and Windows NT® 4 (IIS 4)
- IIS is a secure platform that (when managed) withstands real world attacks
- IIS 6.0 has a much reduced attack surface and a secure set of defaults
- .NET server has a great patch management story
- New authentication and authorization schemes integrated with IIS 6.0
- Great security story for everyone: from hosters to small businesses

Microsoft®

Microsoft Windows.net Server Family